

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

Malikie Innovations Ltd. and Key Patent
Innovations Ltd.

Plaintiff,

v.

Core Scientific, Inc.

Defendant.

§
§
§
§
§
§
§
§
§

Case No. 2:25-cv-00519-JRG-RSP

**DEFENDANT CORE SCIENTIFIC, INC.'S MOTION TO DISMISS
PURSUANT TO FED. R. CIV. P. 12(b)(6) AND 35 U.S.C. § 101**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. STATEMENT OF ISSUES	2
III. BACKGROUND ON THE ASSERTED PATENTS	2
A. Finite Field Calculation Patents (960 and 062 Patents)	3
B. Accelerated Verification Patents (827 and 370 Patents).....	4
C. Improved Montgomery-Style Reduction Patent (286 Patent)	6
IV. LEGAL STANDARD.....	7
A. Patent Eligibility Issues Have Been Repeatedly Determined at the Motion to Dismiss Stage.....	7
B. Claims Directed to Using Mathematical Calculations are Not Patent-Eligible Under <i>Alice/Mayo</i>	8
V. THE CLAIMS OF THE 960 AND 062 PATENTS ARE PATENT INELIGIBLE	11
A. <i>Alice</i> Step 1: The Claims Are Directed to the Abstract Idea of Performing Finite Field Calculations (a Mathematical Formula).....	11
B. <i>Alice</i> Step 2: The Claims Do Not Include an Inventive Concept	16
VI. THE CLAIMS OF THE 827 AND 370 PATENTS ARE PATENT INELIGIBLE	18
A. <i>Alice</i> Step 1: The Claims Are Directed to the Abstract Idea of Generating and Verifying Public Keys in Digital Signatures (a Mathematical Formula).....	18
B. <i>Alice</i> Step 2: The Claims Do Not Include an Inventive Concept	22
C. Claim 1 of the 827 Patent is Also Representative of the 370 Patent Claims	23
VII. THE CLAIMS OF THE 286 PATENT ARE PATENT INELIGIBLE.....	25
A. <i>Alice</i> Step 1: The Claims Are Directed to the Abstract Idea of Modular Reduction (a Mathematical Formula)	25

B. *Alice* Step 2: The Patent Does Not Claim an Inventive Concept..... 28

VIII. CONCLUSION..... 30

TABLE OF AUTHORITIES

Cases

<i>Aatrix Software, Inc. v. Green Shades Software, Inc.</i> , 890 F.3d 1354 (Fed. Cir. 2018)	7
<i>Affinity Labs of Texas v. DIRECTV</i> , 838 F.3d 1253 (Fed. Cir. 2016)	8, 13, 29
<i>Alice Corp. Pty. Ltd. v. CLS Bank Int’l</i> , 573 U.S. 208 (2014)	passim
<i>AML IP, LLC v. Bath & Body Works Direct, Inc.</i> , No. 4:22-CV-216-SDJ, 2024 WL 3825242 (E.D. Tex. Aug. 13, 2024)	8
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	7
<i>Broadband iTV Inc. v. Amazon.com Inc.</i> , 113 F.4th 1359 (Fed. Cir. 2024)	9, 11
<i>BSG Tech LLC v. Buyseasons, Inc.</i> , 899 F.3d 1281 (Fed. Cir. 2018)	13
<i>Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat. Ass’n</i> , 776 F.3d 1343 (Fed. Cir. 2014)	8
<i>Customedia Techs., LLC v. Dish Network Corp.</i> , 951 F.3d 1359 (Fed. Cir. 2020)	10, 21
<i>Diamond v. Chakrabarty</i> , 447 U.S. 303 (1980)	1
<i>Diamond v. Diehr</i> , 450 U.S. 175 (1981)	8
<i>Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.</i> , 758 F.3d 1344 (Fed. Cir. 2014)	12, 19
<i>Elec. Power Grp., LLC v. Alstom S.A.</i> , 830 F.3d 1350 (Fed. Cir. 2016)	8, 11, 17, 24
<i>Enfish, LLC v. Microsoft Corp.</i> , 822 F.3d 1327 (Fed. Cir. 2016)	21
<i>Ericsson Inc. v. TCL Commun. Tech. Holdings Ltd.</i> , 955 F.3d 1317 (Fed. Cir. 2020)	14
<i>First-Class Monitoring, LLC v. United Parcel Serv. of Am., Inc.</i> , 389 F. Supp. 3d 456 (E.D. Tex. 2019)	16, 27
<i>Gottschalk v. Benson</i> , 409 U.S. 63 (1972)	9, 22
<i>In re Board of Trs. of Leland Stanford Junior Univ.</i> , 989 F.3d 1367 (Fed. Cir. 2021)	14, 15, 24, 28

<i>In re Board of Trs. of Leland Stanford Junior Univ.</i> , 991 F.3d 1245 (Fed. Cir. 2021)	passim
<i>In re Comiskey</i> , 554 F.3d 967 (Fed. Cir. 2009)	19
<i>In re TLI Commc’ns LLC Pat. Litig.</i> , 823 F.3d 607 (Fed. Cir. 2016).....	8, 10, 29
<i>Innovations, LLC v. Dexcom, Inc.</i> , 742 F. Supp. 3d 702 (E.D. Tex. 2024).....	8
<i>Intellectual Ventures I LLC v. Cap. One Bank (USA)</i> , 792 F.3d 1363 (Fed. Cir. 2015)	13
<i>Intellectual Ventures I LLC v. Symantec Corp.</i> , 838 F.3d 1307 (Fed. Cir. 2016)	13, 19
<i>Interval Licensing LLC v. AOL, Inc.</i> , 896 F.3d 1335 (Fed. Cir. 2018).....	24
<i>Mackay Radio & Tel. Co. v. Radio Corp. of Am.</i> , 306 U.S. 86 (1939).....	9
<i>Mayo Collaborative Servs. v. Prometheus Lab’ys, Inc.</i> , 566 U.S. 66 (2012).....	9, 10, 22, 26
<i>Optis Cellular Tech., LLC v. Apple Inc.</i> , 139 F.4 th 1363 (Fed. Cir. 2025)	10, 11, 20, 26
<i>Parker v. Flook</i> , 437 U.S. 584 (1978).....	passim
<i>PersonalWeb Techs. LLC v. Google LLC</i> , 8 F.4 th 1310 (Fed. Cir. 2021).....	passim
<i>SAP Am., Inc. v. InvestPic, LLC</i> , 898 F.3d 1161 (Fed. Cir. 2018)	passim
<i>Synopsys, Inc. v. Mentor Graphics Corp.</i> , 839 F.3d 1138 (Fed. Cir. 2016)	14, 21, 27
<i>Torus Ventures LLC v. Cawley Partners, LLC</i> , No. 2:24-CV-00552-JRG, 2025 WL 1799327 (E.D. Tex. June 30, 2025).....	8, 11, 17
<i>Waller v. Hanlon</i> , 922 F.3d 590 (5 th Cir. 2019).....	7

Statutes

35 U.S.C. § 101	passim
-----------------------	--------

Rules

Fed. R. Civ. P. 12(b)(6).....	1, 7
-------------------------------	------

Core Scientific, Inc. (“Core Scientific”) moves to dismiss the Complaint under Fed. R. Civ. P. 12(b)(6) because the claims of the asserted patents are all invalid under 35 U.S.C. § 101. The asserted claims are directed to performing mathematical algorithms using (at most) generic computers. As such, these claims are textbook examples of the kind that the Supreme Court and Federal Circuit have regularly found invalid under § 101.

I. INTRODUCTION

“Einstein could not patent his celebrated law that $E=mc^2$; nor could Newton have patented the law of gravity.” *Diamond v. Chakrabarty*, 447 U.S. 303, 309 (1980). The mass-energy equivalence equation and the law of gravity are mathematical formulas, and mathematical formulas are not patentable. This remains the case today, even with the ubiquity of computers.

Plaintiffs Malikie Innovations Ltd. and Key Patent Innovations Ltd. (“Plaintiffs”) recently purchased a “substantial patent portfolio” from Blackberry Ltd. Dkt. No. 1, ¶ 1. Five of those patents are asserted here. All five patents are generally directed to allegedly improved mathematical algorithms used for, e.g., cryptography functions. All five patents were filed before the Supreme Court’s 2014 decision in *Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 573 U.S. 208 (2014) fundamentally changed the patent eligibility landscape. In the years since, the Federal Circuit has repeatedly held that claims directed to the use of mathematical calculations, even if the solution is for a specific purpose in a specific field of technology, are invalid. *See, e.g., In re Board of Trs. of Leland Stanford Junior Univ.*, 991 F.3d 1245, 1250-51 (Fed. Cir. 2021).

That is precisely the case here. While some of the math disclosed in the patents is complex, that is not enough to save the claims from being found invalid. The mathematical algorithms and calculations claimed can be performed by humans using pencil and paper, and that some of the claims refer to “computer-implemented methods” or using “processors” to do the calculations is unquestionably insufficient as a matter of law. *Alice*, 573 U.S. at 223-224

(rejecting the notion that “generic computer implementations” can “transform a patent-ineligible abstract idea into a patent-eligible invention”). It also does not help Plaintiffs that some of the claims use the algorithms in a specific technology field, for example to verify a “digital signature” used in cryptography, because “limiting the use of an abstract idea ‘to a particular technological environment’” also cannot preserve a claims’ validity. *Id.* at 223.

Resolving the eligibility issues here does not require discovery or claim construction and the issues are thus ripe for consideration. Core Scientific therefore respectfully requests that the Court grant its motion to dismiss the Complaint and hold all claims in the asserted patents invalid under 35 U.S.C. § 101.

II. STATEMENT OF ISSUES

Whether patent claims directed to performing mathematical algorithms—that may include using generic computers to perform the algorithms, and/or perform the algorithms for use in the cryptography field—are directed to non-statutory subject matter and as such should be held invalid under 35 U.S.C. § 101?

III. BACKGROUND ON THE ASSERTED PATENTS

Plaintiffs assert five patents: U.S. Patent Nos. 8,788,827 (the “827 Patent”); 10,284,370 (the “370 Patent”); 7,372,960 (the “960 patent”); 8,666,062 (the 062 Patent”); and 8,532,286 (the “286 Patent”). *See* Dkt. No. 1, Exs. 1-5 respectively.

The 062 Patent is a continuation of the 960 Patent, and both are titled “Method and Apparatus for Performing Finite Field Calculations.” *See id.* Exs. 3, 4. The 370 Patent is a continuation of the 827 Patent, and both are titled “Accelerated Verification of Digital Signatures and Public Keys.” *See id.* Exs. 1, 2. As such, the 960 and 062 Patents are analyzed together herein, as are the 827 and 370 Patents. The remaining patent, the 286 Patent, is titled “System

and Method for Reducing the Computation and Storage Requirements for a Montgomery-Style Reduction.” *Id.*, Ex. 5.

In this case, Plaintiffs assert the patents against the cryptocurrency known as “Bitcoin.” Plaintiffs allege that Bitcoin technology uses elliptical curve cryptography (ECC), and assert that the five patents are directed to improvements in ECC technology. Dkt. No. 1, ¶ 5. The patents are discussed in more detail next.

A. Finite Field Calculation Patents (960 and 062 Patents)

Public key cryptography is a cryptographic method that uses a key pair system. One key, called the public key, encrypts the data. The other key, called the private key, decrypts the data. Public key cryptography can be used in several ways to ensure confidentiality, integrity, and authenticity of digital information, including digital signatures.¹ Public key cryptography has been in use for decades and pre-dates the asserted patents. *See, e.g.,* 960 Patent, 1:17-39 (describing public key cryptography in the *Background of the Invention*).²

A form of public key cryptography known as Elliptic Curve Cryptography (ECC) also pre-dates the patents, with the 960 Patent describing ECC as “a particularly efficient form of public key cryptography.” *Id.*, 1:40-43; *see also* Dkt. 1, ¶¶ 13-14. Generally, as to the public and private keys, larger key sizes provide higher security levels than smaller key sizes, since the time required for an attack on the system depends on the total number of possible keys. 960 Patent, 1:66-2:2. In the context of ECC, different key sizes require different elliptic curves over different finite fields—a set containing a finite number of elements where you can perform addition,

¹ *See* <https://www.cisa.gov/news-events/news/understanding-digital-signatures>. Plaintiffs cite this webpage in the Complaint. Dkt. No. 1, ¶ 12, n. 20.

² Citations are to the 960 Patent for convenience. The 062 Patent has a materially identical specification.

subtraction, multiplication, and division (except by zero), and the results always stay within the set. In a computer, the finite field calculations are computed on machine words—typically 16, 32, or 64 bit representations of numbers stored in memory. *See id.*, 2:2-43. However, the “finite field used in ECC operations are typically 160 bits or more,” and therefore they must be “represented in several machine words.” *Id.*, 2:41-43.

The 960 and 062 Patents recognized that there already existed implementations to perform operations (addition, subtraction, multiplication, division, etc.) on finite fields at the time the patents were filed. *See id.*, 2:25-34. The programs that provided finite field calculations, however, needed to “deal with multiple machine words to complete their calculations.” *Id.*, 2:44-46. It was therefore a goal to “determine the number of words that must be dealt with [] in advance,” such that “more efficient code can be written that expressly deals with exactly the right number of components.” *Id.*, 2:46-50. The alleged invention is directed to performing finite field calculations more efficiently, by representing elements in a fixed number of machine words and reusing “engines” (programs) and optimized multiplication and inversion methods rather than inefficiently using multiple field sizes. *See id.*, Abstract; 4:10-26.³

As explained below, the claims of the 960 and 062 Patents are directed merely at the improved algorithms described in the specification.

B. Accelerated Verification Patents (827 and 370 Patents)

In the *Background of the Invention* section of the 827 Patent, it is acknowledged that public key cryptography can provide “secure communication” over a data communication system “without the necessity to transfer identical keys to other parties in the information

³ The “engines” are “software instructions executed by the processor.” *See* 960 Patent, 6:46-48.

exchange, such as a courier or the like.” 827 Patent, 1:24-28.⁴ Public key cryptography is “based upon the generation of a key pair, one of which is private and the other public that are related by a one way mathematical function.” *Id.*, 1:28-30. Based on the “underlying mathematical structure, the public key is readily computed from the private key but the private key cannot feasibly be ascertained from the public key.” *Id.*, 1:31-34.

Historically, this has enabled users to sign and authenticate messages using the public key. *Id.*, 1:44-48 (“Public key cryptography may also be used to digitally sign a message to authenticate the origin of the message. The author of the message signs the message using his private key and the authenticity of the message may then be verified using the corresponding public key.”).

As the patents acknowledge, the “security of such systems is dependent to a large part on the underlying mathematical structure.” *Id.*, 1:49-50. Accordingly, “various cryptographic algorithms” existed to improve security and “establish common keys for encryption and to perform digital signatures.” *Id.*, 2:22-24. “Such algorithms frequently require the verification of certain operations by comparing a pair of values as to confirm a defined relationship, referred to as the verification equality, between a set of values.” *Id.*, 2:24-27.

The patents note that one such existing algorithm to generate digital signatures is the Elliptic Curve Digital Signature Algorithm (ECDSA). *Id.*, 2:28-30. In ECDSA, for “any message M, the signer can create a signature, which is a pair of integers (r, s) in the case of ECDSA. Any verifier can take the message M, the public key Q, and the signature (r, s), and verify whether it was created by the corresponding signer. This is because creation of a valid signature (r, s) is

⁴ Citations are to the 827 Patent for convenience. The 370 Patent has a materially identical specification.

believed to [be] possible only by an entity who know the private key d corresponding to the public key Q .” *Id.*, 2:42-48.

The patents explain while “ECDSA signature generation is one of the fastest digital signature generation algorithms known,” *id.*, 4:21-22, “ECDSA signature verification is relatively slower.” *Id.*, 4:23-24. The alleged invention is to improve ECDSA verification time, by “enhanc[ing] the efficiency of performing a computation to verify that a value corresponds to the sum of two of the values.” *Id.*, 4:25-33.

As explained below, the claims of the 827 and 370 Patents are directed merely at the improved algorithms described in the specification for the more efficient computation.

C. Improved Montgomery-Style Reduction Patent (286 Patent)

As noted previously, public key cryptography has historically been used to provide data security, integrity and authentication over data communication systems. In public key cryptography, it is often necessary to perform operations including multiplication and exponentiation of integers, where modular arithmetic is used to operate on the integers. 286 Patent, 1:20-23. A part of these operations comprises a calculation called “modular reduction.” *Id.*, 31-32 (“Modular reduction is often employed in cryptographic applications.”). One of the “well-known methods for modular reduction” is called “Montgomery reduction.” *Id.*, 1:32-35. Montgomery reduction “avoids the expensive division operations typically used in classical modular reduction. Montgomery reduction benefits from the fact that steps of multiplication and shifting are generally faster than division on most computing machines.” *Id.*, 1:35-39. Montgomery reduction also “relies on performing certain precomputations and, by doing so, many calculations can be done faster.” *Id.*, 1:39-41.

The purported invention disclosed in the 286 Patent is directed to “improv[ing] the reduction efficiency of a Montgomery machine.” *Id.*, 3:21-26. The patent discloses “an

alternative way in which to produce a Montgomery reduction” by “storing a new precomputed value used to substantially replace the μ and n values used in Montgomery reduction with a single value.” *Id.*, 3:28-31. Through this modification, “the number of multiplications and registers required to effect the Montgomery reduction can be reduced.” *Id.*, 3:40-42.

As explained below, the claims of the 286 Patent are directed merely at the modified algorithm for Montgomery reduction for reducing the number of computations.

IV. LEGAL STANDARD

A. Patent Eligibility Issues Have Been Repeatedly Determined at the Motion to Dismiss Stage

“If patent eligibility is challenged in a motion to dismiss for failure to state a claim pursuant to Rule 12(b)(6), we must apply the well-settled Rule 12(b)(6) standard which is consistently applied in every area of law.” *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 890 F.3d 1354, 1357 (Fed. Cir. 2018). While well-pleaded factual allegations in the complaint are generally accepted as true, no deference is given to unsupported legal conclusions. *Waller v. Hanlon*, 922 F.3d 590, 599 (5th Cir. 2019). Labels and conclusions are not enough, and factual allegations “must be enough to raise a right to relief above the speculative level.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). If the allegations do not raise a claim of entitlement to relief, the complaint must be dismissed. *Id.* at 558.

Patent eligibility under 35 U.S.C. § 101 is a question of law, and the question has been repeatedly resolved on a Rule 12(b)(6) motion “where the undisputed facts, considered under the standards required by that Rule, require a holding of ineligibility under the substantive standards of law.” *SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1166 (Fed. Cir. 2018). Such a decision focuses on the patent itself, especially the specification, without the need of “extraneous fact finding outside the record.” *In re TLI Commc’ns LLC Pat. Litig.*, 823 F.3d 607, 613–14 (Fed. Cir.

2016). Performing claim construction is not a prerequisite for determining patent eligibility. *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat. Ass'n*, 776 F.3d 1343, 1349 (Fed. Cir. 2014). This Court and others in this District have granted motions to dismiss and/or for judgment on the pleadings when the asserted patent failed the patent eligibility test. *See Torus Ventures LLC v. Cawley Partners, LLC*, No. 2:24-CV-00552-JRG, 2025 WL 1799327, at *10 (E.D. Tex. June 30, 2025); *Symbology Innovations, LLC v. Dexcom, Inc.*, 742 F. Supp. 3d 702, 720 (E.D. Tex. 2024) (granting motion for judgment on the pleadings); *AML IP, LLC v. Bath & Body Works Direct, Inc.*, No. 4:22-CV-216-SDJ, 2024 WL 3825242, at *9 (E.D. Tex. Aug. 13, 2024).

B. Claims Directed to Using Mathematical Calculations are Not Patent-Eligible Under *Alice/Mayo*

Section 101 of the Patent Act lists four categories of patent eligible subject matter: “process, machine, manufacture, or composition of matter.” 35 U.S.C. § 101. The Supreme Court has identified three exceptions that do not qualify as patent eligible subject matter: “laws of nature, natural phenomena, and abstract ideas.” *Diamond v. Diehr*, 450 U.S. 175, 185 (1981). In *Alice Corp. Pty. v. CLS Bank Int’l*, the Court established a two-step framework to determine whether patent claims are directed to patent-eligible subject matter. 573 U.S. 208, 217 (2014).

Alice Step One. The first step is to “determine whether the claims at issue are directed to one of those patent-ineligible concepts,” such as an abstract idea. *Id.* At this step, the analysis considers the “focus” of the claims and their “character as a whole.” *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016) (internal quotations and citations omitted). The emphasis is on the “focus of the claimed advance over the prior art to determine if the claim’s character as a whole is directed to excluded subject matter.” *Affinity Labs of Texas v. DIRECTV*, 838 F.3d 1253, 1257 (Fed. Cir. 2016); *Broadband iTV Inc. v. Amazon.com Inc.*, 113

F.4th 1359, 1367 (Fed. Cir. 2024) (“The step one inquiry often turns to the question of what the patent asserts as the claimed advance over the prior art.”).

It is a longstanding rule that “mathematical algorithms for performing calculations, without more, are patent ineligible under § 101.” *In re Board of Trs. of Leland Stanford Junior Univ.*, 991 F.3d 1245, 1250 (Fed. Cir. 2021) (“*Stanford II*”); see *Mackay Radio & Tel. Co. v. Radio Corp. of Am.*, 306 U.S. 86, 94 (1939) (holding that “a scientific truth, or the mathematical expression of it, is not patentable invention”); *Gottschalk v. Benson*, 409 U.S. 63, 72 (1972) (finding claims directed to converting BCD numerals to pure binary numerals ineligible because “the patent would wholly pre-empt the mathematical formula and in practical effect would be a patent on the algorithm itself”); see *Mayo Collaborative Servs. v. Prometheus Lab’ys, Inc.*, 566 U.S. 66, 89 (2012) (establishing a “bright-line prohibition against patenting laws of nature, mathematical formulas, and the like”).

For example, the claim in *Parker v. Flook*, 437 U.S. 584 (1978) was for a method of updating alarm limits in a process for catalytic chemical conversion of hydrocarbons. The method consisted of three steps: an initial step which measured the present value of a process variable, such as the current temperature; an intermediate step which applied an algorithm to calculate an updated alarm-limit value; and a final step in which the actual alarm limit was adjusted to the updated value. *Id.* at 586-87; see *id.* at 596-97 (listing claim). The Court found the claim was not patent eligible. “The process itself, not merely the mathematical algorithm, must be new and useful.” *Id.* at 591. Notably, the “novelty of the mathematical algorithm is not a determining factor at all.” *Id.* Applying the law to the claim, the Court found that the claimed process “simply provides a new and presumably better method for calculating alarm limit values.” *Id.* at 594–95. But a “claim for an improved method of calculation, even when tied to a

specific end use, is unpatentable subject matter under § 101.” *Id.* at 595 n.18; *see also Optis Cellular Tech., LLC v. Apple Inc.*, 139 F.4th 1363, 1379 (Fed. Cir. 2025) (“We conclude that the claims are directed to an abstract idea—a mathematical formula.”).

Alice Step Two. If, at step one, the claims fall within one of the exceptions, the analysis moves to step two and considers the “elements of each claim both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent-eligible application.” *Alice*, 573 U.S. at 217. The second step focuses on searching for “an inventive concept—i.e., an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself.” *Id.* at 217–18.

Transformation into a patent-eligible application requires “more than simply stat[ing] the [abstract idea] while adding the words ‘apply it.’” *Id.* at 221 (*citing Mayo*, 566 U.S. at 72). “[W]ell-understood, routine, conventional” activities normally are not sufficient to transform an abstract idea into a patent-eligible application. *Mayo*, 566 U.S. at 79. In the context of computer-related technology, the claim must be directed to an improvement in the functionality of the computer or network platform itself, rather than an improvement of an abstract process by invoking a computer merely as a tool. *Customedia Techs., LLC v. Dish Network Corp.*, 951 F.3d 1359, 1364 (Fed. Cir. 2020); *Alice*, 573 U.S. at 223–26 (holding that “mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention” and finding the claimed structures “‘data processing system,’ ‘communications controller,’ and ‘data storage unit’ [were] purely functional and generic”); *TLI*, 823 F.3d at 614 (holding that “generic computer components [are] insufficient to add an inventive concept to an otherwise abstract idea”).

Finally, the Federal Circuit has explained that the two *Alice* steps are plainly related: “many of our opinions make clear that the two stages involve overlapping scrutiny of the content of the claims....” *Elec. Power Group*, 830 F.3d at 1353; *Broadband iTV*, 113 F.4th at 1369 (“We have observed that steps one and two are ‘plainly related’ and patent eligibility may ‘involve overlapping scrutiny of the content of the claims’.... [I]t may be necessary to analyze conventionality at step one as well as step two, such as to determine whether a claim is directed to a longstanding or fundamental human practice or to determine what the patent asserts is the claimed advance over the prior art.”).

V. THE CLAIMS OF THE 960 AND 062 PATENTS ARE PATENT INELIGIBLE

A. *Alice* Step 1: The Claims Are Directed to the Abstract Idea of Performing Finite Field Calculations (a Mathematical Formula)

The 960 and 062 Patents, which both issued prior to *Alice*, claim nothing more than the abstract idea of performing finite field calculations to obtain a reduced result. *See* representative claim below. This is a mathematical formula like that the Federal Circuit has classified as abstract. *Optis Cellular*, 139 F.4th at 1379. The claims are directed to performing mathematical tasks that humans could perform using pencil and paper. *See Broadband iTV*, 113 F.4th at 1371 (stating that the claims included steps that “can be performed in the human mind or using a pencil and paper. This is another indication that the claims are abstract.”); *Torus Ventures*, No. 2:24-CV-00552-JRG, 2025 WL 1799327, at *6 (finding a claim was directed to the abstract idea of ‘encrypting a bit stream of data that has already been encrypted and associated its decryption algorithm’ and holding that the “Court’s conclusion is further supported by the fact that the operative steps of the claim can be performed by a human with pen and paper”).

Claim 3 of the 960 Patent is exemplary. It is directed to a five-step method:

3. A method of performing a finite field operation on elements of a finite field, comprising the steps of

- a) representing each element as a predetermined number of machine words;
- b) performing a non-reducing wordsized operation on said representations, said wordsized operation corresponding to said finite field operation;
- c) completing said non-reducing wordsized operation for each word of said representations to obtain an unreduced result;
- d) upon computing said unreduced result, performing a specific modular reduction of said unreduced result to reduce said unreduced result to that of a field element of said finite field to obtain a reduced result; and
- e) using said reduced result in a cryptographic operation.

Claim 3 is directed at a method of performing a mathematical operation, specifically a finite field operation on “elements” to obtain a “reduced result.”⁵ This is a patent-ineligible abstract idea. *See Stanford II*, 991 F.3d at 1250 (finding that the claims were “directed to patent ineligible abstract ideas. Specifically, the claims are directed to the use of mathematical calculations and statistical modeling”). The Federal Circuit has ruled many times that “[w]ithout additional limitations, a process that employs mathematical algorithms to manipulate existing information to generate additional information is not patent eligible.” *Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.*, 758 F.3d 1344, 1351 (Fed. Cir. 2014). That is what claim 3 does—it manipulates existing information (“elements” in the form of a “predetermined number of machine words”) by performing/computing certain operations to arrive at additional information (a “reduced result”). The claimed steps can be “performed by a human, mentally or

⁵ The claim specifies that the “elements” are represented as a predetermined number of machine words. The specification states that the elements “may be represented as polynomials with binary coefficients, which may be represented as bits in hardware or software,” or simply as “integers.” *See* 960 Patent, 2:25-33. The elements therefore comprise data.

with pen and paper,” demonstrating their ineligibility. *Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1318 (Fed. Cir. 2016).

In *Stanford II*, the Federal Circuit analyzed an analogous claim: one drawn to a “computerized method of inferring haplotype phase in a collection of unrelated individuals” that included “receiving” and “storing” genotype data, “imputing an initial haplotype phase for each individual ... based on a statistical model,” “building a data structure” that included “re-computation of [a] set of parameters” contained within the data structure,” and other calculation and storage steps. 991 F.3d at 1248. The court held that “the claims are directed to the use of mathematical calculations and statistical modeling” and thus are directed to patent ineligible abstract ideas. *Id.* at 1250.⁶

The presence in claim 3 of the step of “using said reduced result in a cryptographic operation” does not save the claim. “An abstract idea does not become nonabstract by limiting the invention to a particular field of use or technological environment, such as the Internet.” *Intellectual Ventures I LLC v. Cap. One Bank (USA)*, 792 F.3d 1363, 1364 (Fed. Cir. 2015). As the Federal Circuit has held, a limitation which “confine[s] the abstract idea to a particular technological environment ... does not render the claims any less abstract.” *Affinity Labs*, 838 F.3d at 1258-59 (collecting cases). That applies here. Limiting the “reduced result” generated by the mathematical calculations to use in a “cryptographic operation” does not transform the claim into a non-abstract idea. A “claim is not patent eligible merely because it applies an abstract idea in a narrow way.” *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1287 (Fed. Cir. 2018).

⁶ Indeed, the claims in *Stanford II* are more detailed than those here and required use of a computer system with a processor and memory (*see* 991 F.3d at 1248), which are wholly lacking from claim 3. And regardless, those generic computer components did not alter the Federal Circuit’s analysis or conclusion.

In the Complaint, Plaintiffs characterize the inventions in the 960 and 062 Patents as providing “technological benefits” that result in “shorter processing time and fewer processor operations.” Dkt. No. 1, ¶¶ 91-92; *see also* 960 Patent, 4:24-26 (“In this way, fast engines can be produced for many specific finite fields, without duplicating the bulk of the engine instructions (program).”).

Even taking those representations as true, it does not impact the analysis. First, the claim does not require “fast engines” or “many specific finite fields.” *See Ericsson Inc. v. TCL Commun. Tech. Holdings Ltd.*, 955 F.3d 1317, 1328-29 (Fed. Cir. 2020) (holding that details from the specification cannot be imported into the claims when considering the abstract idea analysis: “this allegedly novel aspect of the invention is wholly missing” from the claims). As noted above, claim 3 is so broad as to be capable of being performed with pencil and paper.

Further, even if the claimed invention results in an improved way to perform finite field operations, that is not enough to impart eligibility. “Even accepting the argument that the claimed process results in improved data, we are not persuaded that claim 1 is not directed to an abstract mathematical calculation.” *In re Board of Trs. of Leland Stanford Junior Univ.*, 989 F.3d 1367, 1373 (Fed. Cir. 2021) (“*Stanford I*”); *see Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1151 (Fed. Cir. 2016) (“[A] claim for a new abstract idea is still an abstract idea.”).

Claim 3 is therefore directed to an abstract idea. The same analysis applies to the other claims in the 960 and 062 Patents. As to the 960 Patent, each of the other independent claims (1, 2, 4, 5) applies some subset of the same steps of using a machine word representation, performing finite field operations on the words and performing a reduction on the words to obtain a reduced result. *See* claim 1 (“reduced result”); claim 2 (“reduce said unreduced intermediate product to that of a field element”); claim 4 (same); claim 5 (“obtain a reduced

result”). While exemplary claim 3 outlines the operation for a general finite field operation, claims 1 and 2 describe addition and multiplication respectively, which are still mathematical computations that can be performed by humans. Claim 4 is an even more generalized version, utilizing subsets rather than words computed by a processor. Claim 5 adds that the finite fields are paired with elliptic curves. Every claim is directed to performing mathematical calculations, which are abstract ideas.⁷

The dependent claims likewise add nothing other than further details of the mathematical formula. They specify that the modular reduction “is determined by said finite field” (claim 6), the finite field operation is addition (claim 7), subtraction (claim 8) or multiplication (claim 9). These merely specify the type of math performed, and do not make the claims any less abstract.

As to the 062 Patent, claim 1 closely tracks claim 3 of the 960 Patent, only specifying that the method is performed by “a processor.” This recitation of using a generic processor to perform the algorithm does not alter the analysis. *See, e.g., Stanford I*, 989 F.3d at 1372 (finding that claims requiring “using a computer system comprising a processor and memory” to perform mathematical operations were patent ineligible). Independent claim 8 is directed to a “non-transitory computer readable medium comprising computer executable instructions for performing a finite field operation,” and independent claim 15 similarly is directed to a “cryptographic engine comprising a processor and memory ... comprising instructions.”

Otherwise, both claims likewise track claim 3 of the 960 Patent. The dependent claims of the 062

⁷ To the extent the claims include an “engine” (claim 4) or “finite field multipliers” and “finite field reducer[s]” (claim 2), these are the names for the generic processors or programs (source code) used to carry out the mathematical calculations. *See* 960 Patent, 2:37-46 (describing “a general purpose computational engine (for example a typical CPU)” and (“[e]ngine routines (programs)”; 4:12-26; 6:45-48 (“The processor [] operates to execute an appropriate engine ... on the data. The engines may be software instructions executed by the processor, or they may have dedicated coprocessors.”).

Patent add further details regarding the mathematical calculations performed. These limitations are not significantly more than the abstract idea identified in the 960 Patent, claim 3.

B. *Alice* Step 2: The Claims Do Not Include an Inventive Concept

Turning to the second step of the *Alice* test, the Court considers the limitations of the claims, other than the abstract idea, to determine whether they contain an “inventive concept” sufficient to transform the abstract idea into a patent-eligible application. *Alice*, 573 U.S. at 217. As discussed above, representative claim 3 of the 960 Patent recites a five-step method: (1) a representation as “a predetermined number of machine words”; (2) performing a non-reducing finite field operation on said representation; (3) completing the operation for each word; (4) performing modular reduction to obtain a reduced result; and (5) using the result in a cryptographic operation. There is nothing in the claim other than the steps of the mathematical algorithm. As such, the claim fails *Alice* step two because the limitations “add nothing outside the abstract realm.” *SAP*, 898 F.3d at 1169.

Limiting the claim to using the reduced result “in a cryptographic operation” does not change the analysis. The Supreme Court in *Alice* made it clear that simply adding “apply it” to an abstract idea does not transform the claim into a patent eligible application. 573 U.S. at 221. Here, the 960 Patent admits that finite field operations were used in cryptographic operations before the alleged invention. 960 Patent, 1:45-2:26. Thus, there is nothing “significantly more” in the claims beyond the abstract idea itself. *See First-Class Monitoring, LLC v. United Parcel Serv. of Am., Inc.*, 389 F. Supp. 3d 456, 471 (E.D. Tex. 2019) (Bryson, J., sitting by designation) (“That is, the assertedly ‘inventive concept’ is the abstract idea itself. As noted, however, the ‘inventive concept’ element of the section 101 analysis requires ‘significantly more’ than the abstract idea itself.”). It does not matter whether the mathematical calculations in the claim improve on what existed previously (a point which Core Scientific does not concede). *See Torus*

Ventures, No. 2:24-CV-00552-JRG, 2025 WL 1799327, at *10 (“Even if the Court were to accept [patentee’s] view that these particular ideas are not well-known, routine, or conventional, the Court would still be compelled to find that a ‘claim for a new abstract idea is still an abstract idea.’”) (citing *PersonalWeb Techs. LLC v. Google LLC*, 8 F.4th 1310, 1318 (Fed. Cir. 2021)).⁸

Claim 3 therefore fails both parts of the *Alice* test and should be found invalid under § 101.

The analysis of *Alice* Step 2 is the same for the other claims of the 960 and 062 Patents. Some independent claims recite “a processor” (960, claims 2, 4, 5), “an accumulator” and “registers” (960, claim 1), and “processor and memory” (062, claim 15). However, as the Federal Circuit in *SAP* found, “[s]ome of the claims require various databases and processors, which are in the physical realm of things. But it is clear, from the claims themselves and the specification, that these limitations require no improved computer resources [the patent owner] claims to have invented, just already available computers, with their already available basic functions, to use as tools in executing the claimed process.” 898 F.3d at 1169–70. The 960 Patent does not disclose any specific improvements to the processor, accumulator, or registers themselves, but, as illustrated above, is directed to more efficient finite field calculations, which are purely mathematical in nature. Therefore, “such invocations of computers and networks that are not even arguably inventive are insufficient to pass the test of an inventive concept in the application of an abstract idea.” *Elec. Power Grp.*, 830 F.3d at 1355; *PersonalWeb*, 8 F.4th at 1319 (“[M]erely adding computer functionality to increase the speed or efficiency of the process does not confer patent eligibility on an otherwise abstract idea.”).

⁸ The Supreme Court has held that the “novelty of the mathematical algorithm is not a determining factor at all.... [I]t is treated as though it were a familiar part of the prior art.” *Flook*, 437 U.S. at 591.

Accordingly, the claims of the 960 and 062 Patent do not qualify for patent protection, and as such should be found invalid under § 101.

VI. THE CLAIMS OF THE 827 AND 370 PATENTS ARE PATENT INELIGIBLE

A. *Alice* Step 1: The Claims Are Directed to the Abstract Idea of Generating and Verifying Public Keys in Digital Signatures (a Mathematical Formula)

The 827 and 370 Patents claim nothing more than the abstract idea of recovering a public key from a signature—a mathematical formula that humans could perform with pencil and paper which is merely sped up by a computer.

The patents describe the invention as “verifying the equality of a relationship between the sum of scalar multiples of a pair of points on an elliptic curve and a third point on said curve.” 827 Patent, 4:38-40. The patent explains, “there is a need to enhance the efficiency of performing a computation to verify that a value corresponds to the sum of two of the values [and it is] an object of the presentation invention to obviate or mitigate the [current] disadvantages.” *Id.*, 4:28-32. The method comprises three steps: (1) “obtaining a pair of integers” related by one of several scalars; (2) obtaining an equivalent relationship between the integers from the relationship between the scalars (3) computing the relationship to verify the equality. *Id.*, 4:40-47. Claim 1 of the 827 Patent recites “[a] computer-implemented method” performing these steps:

1. A computer-implemented method comprising:

receiving, from a signer, a signature on a message M, wherein the signature includes a first signature component r and a second signature component s;

obtaining an elliptic curve point associated with the first signature component r;
and

generating, by operation of a cryptographic module comprising one or more processors, a public key of the signer based on the elliptic curve point and a hash value e computed from the message M:

wherein the elliptic curve point comprises a first elliptic curve point R, the public key of the signer comprises a second elliptic curve point Q, generating the public key of the signer comprises computing $Q=r^{-1}(sR-eG)$, and G comprises a generator of an elliptic curve group that includes the first elliptic curve point R and the second elliptic curve point Q.

The three steps in claim 1 are performed within the “context of an algorithm such as the ECDSA.” *Id.*, 4:63.

Claim 1 is therefore directed to the abstract idea of performing mathematical calculations to generate a public key of a signer—a mathematical formula. With the “exception of generic computer-implemented steps, there is nothing in the claims themselves that foreclose them from being performed by a human.” *Symantec*, 838 F.3d at 1318; *see In re Comiskey*, 554 F.3d 967, 979 (Fed. Cir. 2009) (holding that “mental processes—or processes of human thinking—standing alone are not patentable even if they have practical application.”). Further, as with analysis of the 960 and 062 Patents above, using mathematical algorithms on existing information to generate additional information is not patent eligible. *Digitech*, 758 F.3d at 1351. In *Digitech*, the claim recited a “process of taking two data sets and combining them into a single data set, the device profile. The two data sets are generated by taking existing information...and organizing this information into a new form.” *Id.* The Federal Circuit held that such a “claim thus recites an ineligible abstract process of gathering and combining data that does not require input from a physical device.” *Id.* Similarly, claim 1 of the 827 Patent merely recites a method of calculating the public key from existing information (the signature components). Therefore, claim 1 is also directed to an abstract idea.

Claim 1 is much like the claim the Supreme Court found invalid in *Parker v. Flook*. That claim is reproduced below:

1. A method for updating the value of at least one alarm limit on at least one process variable involved in a process comprising the catalytic chemical conversion of hydrocarbons wherein said alarm limit has a current value of

$Bo+K$

wherein Bo is the current alarm base and K is a predetermined alarm offset which comprises:

(1) Determining the present value of said process variable, said present value being defined as PVL ;

Determining a new alarm base $B1$, using the following equation:

$$B[1]=Bo(1.0<v1>minF)+PVL(F)$$

where F is a predetermined number greater than zero and less than 1.0;

(3) Determining an updated alarm limit which is defined as $B1+GK$; and thereafter

(4) Adjusting said alarm limit to said updated alarm limit value.

The Court found this claim invalid: “if a claim is directed essentially to a method of calculating, using a mathematical formula, *even if* the solution is for a specific purpose, the claimed method is nonstatutory.” *Flook*, 437 U.S. at 595 (emphasis added). Claim 1 of the 827 Patent is also nonstatutory, because it is directed to using the mathematical formula $Q=r^{-1}(sR-eG)$ from existing information (a signature) to generate additional information (a public key).⁹ That it may do so to generate a public key is of no moment because using the algorithm for a “specific purpose” is not enough. *Id.*; see also *Stanford II*, 991 F.3d at 1250.

That claim 1 requires a “computer-implemented” method and has “a plurality of processors” does not change the analysis. “[I]mplementing and processing calculations with a

⁹ Claim 1 is also much like the one the Federal Circuit found was directed to an abstract idea (a mathematical formula) in *Optis Cellular*. See 139 F.4th at 1378.

regular computer does not change the character of [the] claim ... from an abstract idea into a practical application.” *Id.*¹⁰ Indeed, claim 1 does not recite any “specific improvement to the way computers operate.” *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1336 (Fed. Cir. 2016). It simply describes steps or operations to be performed—i.e., “receiving,” “obtaining,” “generating,” “computing”—and the relationships between mathematical objects—i.e., “elliptic curve points,” “signature component[s],” and “hash values.”

Plaintiffs again allege that the 827 and 370 Patents provide a “technological improvement” to the ECDSA digital signature verification process by enabling “accelerated signature verification.” Dkt. 1, ¶ 74. Similarly, the specification alleges that “the efficiency of verifying of ECDSA signatures is particularly desirable” and it is an “object of the present invention to obviate or mitigate” disadvantages with current methods. 827 Patent, 4:18-19, 4:30-32). But the claims do not specify any improved speed or efficiency. At any rate, any “improved speed or efficiency inherent with applying the abstract idea on a computer” is not enough under *Alice* Step One. *Customedia*, 951 F.3d at 1364; *PersonalWeb*, 8 F.4th at 1319. And as already explained, even assuming that the underlying mathematical algorithm specified in the claims may be an improvement over earlier iterations, a “claim for a new abstract idea is still an abstract idea.” *Synopsis*, 839 F.3d at 1151. Thus, claim 1 is directed to an abstract idea.

Claim 1 is representative of the other 827 Patent claims. Independent claim 6 simply adds that the steps are “executed by one or more processors.” Independent claim 10 requires “[a] computing device” that performs the steps. The dependent claims add nothing of significance. They require verifying the generated key represents the public key (claim 2, 7, 11), adding a

¹⁰ In *Flook*, the Supreme Court recognized that the claim was intended to be performed through “the use of computers,” but that did not change the analysis. 437 U.S. at 595.

cofactor to the first elliptic curve point (claim 3, 8, 12), stating the public key can be used to verify the signature (claim 4, 9, 13), and verifying the signature according to an ECDSA (claim 5). These limitations, directed to further details of the algorithm or to the field of use, do not make the claims any less abstract and confirm that claim 1 is representative.

B. *Alice* Step 2: The Claims Do Not Include an Inventive Concept

The claims also fail *Alice* step two because there is nothing else in the claim transforming the claim into a patent eligible application. As before, aside from the generic “one or more processors,” there is nothing in the claim other than the citation of the steps of the mathematical algorithm. The claim therefore fails *Alice* step two because the limitations “add nothing outside the abstract realm.” *SAP*, 898 F.3d at 1169; *PersonalWeb*, 8 F.4th at 1319 (find that “there is nothing ‘inventive’ about any claim details, individually or in combination, that are not themselves abstract ideas”). In *Benson*, the claim was directed to converting one form of numerical representation to another and the patent applicant invoked a “general-purpose digital computer” to carry out the task. 409 U.S. at 65. But the computer implementation did not provide the necessary inventive concept as the Supreme Court held that “mathematical procedures can be carried out in existing computers long in use, no new machinery being necessary.” *Id.* at 67; *see Mayo*, 566 U.S. at 84 (“simply implementing a mathematical principle on a physical machine, namely a computer, was not a patentable application of that principle.”).

The dependent claims also do not add “significantly more” to the abstract idea. Integrating more elliptic curves, using cofactors, and verifying signatures of the message according to an ECDSA are merely further details in the algorithm and/or are not new features. 828 Patent, claims 3, 8, 12 (“the first elliptic curve point R is generated based on the first signature component r and a cofactor h for an elliptic curve”); claims 2, 7, 11 (“verifying that the second elliptic curve point Q represents the public key of the signer”); claims 4, 9, 13 (“the

public key of the signer can be used to verify the signature”); claim 5 (“verifying the signature comprises verifying the signature according to an Elliptic Curve Digital Signature Algorithm (ECDSA)”). *See, e.g.,* 827 Patent, 2:28-41-63. Thus, the claims are all invalid.

C. Claim 1 of the 827 Patent is Also Representative of the 370 Patent Claims

The claims in the 370 Patent include 3 independent claims and 8 dependent claims. Claim 1 of the 370 Patent is like claim 1 of the 827 Patent:

1. A method performed by a hardware processor of a computing device, comprising:

receiving, by a receiver of the computing device and through a network, an electronic message including a signature, wherein the electronic message omits a public key of a signer, and the signature comprises a signature on the electronic message M;

receiving, by the receiver of the computing device and through the network, a first elliptic curve point associated with a signature component from the signer, wherein the signature component comprises a first signature component r, the signature includes the first signature component r and a second signature component s, and the first elliptic curve point comprises an elliptic curve point R;

recovering, by the hardware processor of the computing device, the omitted public key of the signer based on the received first elliptic curve point and the received signature, wherein the public key comprises a second elliptic curve point in an elliptic curve group different from the first elliptic curve point, wherein the elliptic curve group includes the first and second elliptic curve points, wherein the second elliptic curve point comprises an elliptic curve point Q, wherein recovering the omitted public key of the signer comprises computing $Q = r^{-1}(sR - eG)$, wherein G comprises a generator of an elliptic curve group that includes the elliptic curve point R and the elliptic curve point Q, and wherein e is a hash value computed from the electronic message M; and

verifying, by the hardware processor of the computing device, the received signature using the recovered public key which provides an accelerated verification of the received signature.

Claim 1 thus recites materially the same steps of 827 Patent claim 1, and adds the limitation of using the public key for verification. But this latter step is acknowledged to have

been routine in cryptography. 370 Patent, 2:32-45; 3:1-9. Thus, it does not change the analysis concerning whether the claim is directed to an abstract idea.

Claim 1 also specifies generic computing components (“computing device,” “hardware processor,” “network”). It is beyond debate that such limitations cannot convert an abstract claim into a non-abstract one. *Interval Licensing LLC v. AOL, Inc.*, 896 F.3d 1335, 1345 (Fed. Cir. 2018) (finding claims abstract when they offer “nothing more than generic, pre-existing computer functionality” to perform the abstract idea).

Nor do these generic limitations save the claim under *Alice* Step Two. *See Elec. Power Grp.*, 830 F.3d at 1355 (“The claims at issue do not require any nonconventional computer, network, or display components, or even a ‘non-conventional and non-generic arrangement of known, conventional pieces,’ but merely call for performance of the claimed information collection, analysis, and display functions ‘on a set of generic computer components’....”) (citations omitted); *Stanford I*, 989 F.3d at 1374 (stating that “it is hard to imagine a patent claim that recites hardware limitations in more generic terms than the terms employed by claim 1 [‘computer with a ‘processor’ and a ‘memory’]; *see also Alice*, 573 U.S. at 226 (explaining that the hardware-related terms ‘data processing system,’ ‘communications controller,’ and ‘data storage unit’ are ‘purely functional and generic’)).

Thus, claim 1 of the 370 Patent is also invalid for failing to claim patent-eligible subject matter.

The remaining independent claims (6 and 10) recite the same steps as claim 1, but in the context of (1) a non-transitory computer readable medium and processors (claim 6) and (2) a computing device (claim 10). As with claim 1, these limitations do not change the analysis as a

“mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention.” *Alice*, 573 U.S. at 223.

The dependent claims of the 370 Patent match those of the 287 Patent: verifying that Q is the public key (claims 2, 7, 11), the elliptic curve point R generated based on r and a cofactor h (claims 3, 8), use of public key in signature verification (claims 4, 9), and the verification based on ECDSA (claim 5). *See* Section VI.B *supra*. Therefore, claim 1 of the 370 Patent is representative of all claims in the patent, and as claim 1 fails the two-step test under *Alice*, all claims in the 370 Patent should be held invalid under 35 U.S.C. § 101.

VII. THE CLAIMS OF THE 286 PATENT ARE PATENT INELIGIBLE

A. *Alice* Step 1: The Claims Are Directed to the Abstract Idea of Modular Reduction (a Mathematical Formula)

The 286 Patent is based around the well-known Montgomery-style reduction and discloses an alleged improved method of Montgomery-style reduction based on a precomputed value. 286 Patent, 1:32-35 (“Of the well known method for modular reduction, the most commonly used is the method of Montgomery modular reduction, referred to as Montgomery reduction in short”). Representative claim 1 recites a 3-step process: (1) obtaining an operand; (2) computing a new operand using a reduction value; (3) outputting the new operand:

1. A method for performing, on a cryptographic apparatus, a Montgomery-style reduction in a cryptographic operation, the method comprising:
obtaining an operand for the cryptographic operation;

computing a modified operand using a reduction value, instead of a modulus used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof, the reduction value being a function of the modulus; and

outputting the modified operand.

Claim 1 is directed to an abstract idea of using a mathematical algorithm (formula) to perform a form of Montgomery reduction. It is acknowledged in the patent that “modular

arithmetic is used to operate on the integers” in cryptography and one classical example is “to multiply two numbers modulo n .” 286 Patent, 1:20-30. The approach to this calculation is “to first perform the multiplication and then calculate the remainder...The calculation of the remainder is referred to as reduction in modular arithmetic.” *Id.* Montgomery reduction was one of the most used methods for modular reduction. *Id.*, 1:31-46. As such, a form of Montgomery style reduction is an abstract idea. *See Mayo*, 566 U.S. at 89 (holding there is “a bright-line prohibition against patenting laws of nature, mathematical formulas, and the like”); *Flook*, 437 U.S. at 591 (holding that “the process itself, not merely the mathematical algorithm, must be new and useful”); *SAP*, 898 F.3d at 1167 (analyzing information by mathematical algorithms without more is directed to an abstract idea); *Optis Cellular*, 139 F.4th at 1379 (“We conclude that the claims are directed to an abstract idea—a mathematical formula.”).

Applying the Montgomery reduction on a “cryptographic apparatus” or as part of a “cryptographic operation” does not make the abstract idea any less abstract. First, Montgomery reduction was a well-understood technique used in cryptography before the patent. 286 Patent, 1:31-46. The patent confirms that a “cryptographic apparatus” is generic hardware and/or software. 286 Patent, 4:2-5 (“It will be appreciated that the cryptographic module [] and any component thereof may be implemented as an apparatus in hardware or in software (computer readable instructions embodied in/on a computer readable medium.”). Second, “a claim for an improved method of calculation, even when tied to a specific end use, is unpatentable subject matter under § 101.” *Flook*, 437 U.S. at 595 n.18

Plaintiffs again allege in the Complaint that the 286 Patent provides solutions to “technical problems.” Dkt. No. 1, ¶ 103. But the alleged improvements are to the Montgomery reduction algorithm itself, which is not enough to overcome *Alice* Step One. Even assuming

arguendo the proposed method in the patent yields a more efficient Montgomery reduction by reducing the number of multiplications and registers previously needed, the “improvement in computational accuracy alleged here does not qualify as an improvement to a technological process; rather, it is merely an enhancement to the abstract mathematical calculation of haplotype phase itself.” *Stanford II*, 991 F.3d at 1251; *see also First-Class Monitoring*, 389 F. Supp.3d at 462 (“Nor does the fact that a computer can perform such operations more rapidly and efficiently make an abstract idea any less abstract or any more patent-eligible.”) (collecting cases). That applies here. An improved Montgomery reduction algorithm that performs calculations more efficiently is still an algorithm and thus an abstract idea. *See* 286 Patent, 3:21-22 (stating that the objective of the invention is “to improve the reduction efficiency of a Montgomery machine”). Therefore, the improvements here are enhancements to the ineligible concept and are not eligible for patent protection. *See Synopsys*, 839 F.3d at 1151 (“[A] claim for a new abstract idea is still an abstract idea”).¹¹

Claim 1 is representative of the remaining claims. The other independent claims (10, 18) are materially identical to claim 1, specifying only “computer executable instructions ... executed by [a] processor” (claim 10) or “computer executable instructions” on a “non-transitory computer readable medium” (claim 18). The three algorithmic steps in both claims are otherwise materially identical to the ones in claim 1. The dependent claims add nothing more than additional details to the algorithm: providing the equation of n' (claims 2, 11, 19), further

¹¹ None of the 286 Patent claims refer to a reduction in the number of registers needed. The only claims that specify registers are dependent claims 4, 13, and 21. But those claims only add details regarding performing a “standard Montgomery reduction,” which was admittedly in the prior art. 286 Patent, 1:31-34 (“Modular reduction is often employed in cryptographic applications. Of the well known methods for modular reduction, the most commonly used is the method of Montgomery modular reduction, referred to as Montgomery reduction in short.”).

replacing words of the operand using a reduction value (claims 3, 12, 20), discussing the steps of a standard Montgomery reduction (claims 4, 13, 21), use of a Montgomery engine (claim 5),¹² identifying that the reduction value is pre-computed (claims 6, 14, 22), shifting words of the operand (claims 7, 15, 23), adding a carry to the output if a carry is produced (claims 8, 16, 24), and listing multiplication or squaring as cryptographic operation (claims 9, 17, 25). These limitations are directed at additional steps or details of the method Montgomery reduction, do not make the claims any less abstract, and confirm that claim 1 is representative.

B. *Alice* Step 2: The Patent Does Not Claim an Inventive Concept

Claim 1 also fails *Alice* step 2. At this step, the analysis focuses on limitations of the claim both individually and combined to determine whether the additional limitations transform the claim into a patent-eligible application. *Alice*, 573 U.S. at 217. Here, the entirety of the claim is directed at the allegedly improved Montgomery reduction algorithm. The recited steps are (1) obtaining data (an “operand”); (2) modifying data with the mathematical algorithm (“computing a modified operand”); and (3) outputting data (“the modified operand”). *See Stanford I*, 989 F.3d at 1374 (finding claim failed *Alice* step 2: “claim 1 ends at storing the haplotype phase and ‘providing’ it ‘in response to a request.’ Simply storing information and providing it upon request does not alone transform the abstract idea into patent eligible subject matter.”). This is not materially different from claim 1’s steps of modifying and outputting data. Even if the claim captures improvements in the Montgomery reduction algorithm (which Core Scientific does not

¹² The “Montgomery engine” is generic hardware or software configured to perform the algorithm and was admitted prior art in the 286 Patent. *See* 286 Patent, 1:65-2:3 (“[A] computational engine may be used for calculating the Montgomery product of two numbers, this engine being sometimes referred to as a Montgomery engine or Montgomery machine. The engine may be implemented in a hardware or software module and operates on a set of parameters to produce a result.”); *id.*, 4:2-5.

concede), the fact that “some of those [claimed] steps had not previously been employed in the art was not sufficient, standing alone, ‘to confer patent eligibility upon the claims at issue.’”

Affinity Labs, 838 F.3d at 1263 (quoting *Alice*); see also *Stanford II*, 991 F.3d at 1252 (holding that novelty is not the “touchstone of patent eligibility. That a specific or different combination of mathematical steps yields more accurate haplotype predictions than previously achievable under the prior art is not enough to transform the abstract idea in claim 1 into a patent eligible application”); *PersonalWeb*, 8 F.4th at 1319.

The outcome is the same for the independent claims (10 and 18). Inclusion of generic computer components does not change the Step Two analysis. See *Stanford II*, 991 F.3d at 1252 (“Nor does claim 1 require or result in a specialized computer or a computer with a specialized memory or processor. Indeed, it is hard to imagine a patent claim that recites hardware limitations in more generic terms than the terms employed by claim 1” where the claimed method steps were carried out by a “computer system” with a “processor” and a “memory”).

Additional limitations in the dependent claims also do not add any inventive concepts. They either add further features related to the abstract idea (the variation of the Montgomery reduction) itself, such as providing the equation of n' (claims 2, 11, 19), further replacing words of the operand using a reduction value (claims 3, 12, 20), discussing the steps of a standard Montgomery reduction (claims 4, 13, 21), identifying that the reduction value is pre-computed (claims 6, 14, 22), shifting words of the operand (claims 7, 15, 23), adding a carry to the output if a carry is produced (claims 8, 16, 24), and listing multiplication or squaring as cryptographic operation (claims 9, 17, 25), or reciting a generic computer component such as the use of a Montgomery engine (claim 5). *TLI*, 823 F.3d at 614 (“our precedent[s] find[] generic computer components insufficient to add an inventive concept to an otherwise abstract idea”);

PersonalWeb, 8 F.4th at 1319 (“[O]ur precedent is clear that merely adding computer functionality to increase the speed or efficiency of the process does not confer patent eligibility on an otherwise abstract idea.”).

Because all claims of the 286 Patent fail the two-step test under *Alice*, the claims should be held invalid under 35 U.S.C. § 101.

VIII. CONCLUSION

Core Scientific respectfully requests that the Court grant its motion to dismiss Plaintiffs’ Complaint. The claims of each patent are directed to abstract concepts ineligible for patent protection under 35 U.S.C. § 101. The claims describe mathematical algorithms that humans could perform using pencil and paper, and at most add generic computer components functioning in a conventional way. Resolving these eligibility issues does not require discovery or claim construction and is ripe for consideration now.

[CERTIFICATION OF COMPLIANCE FOLLOWS SIGNATURE BLOCK]

Dated: July 20, 2025

Respectfully submitted,

/s/ Brian E. Ferguson

Brian E. Ferguson
WINSTON & STRAWN LLP
1901 L Street, N.W.
Washington, D.C. 20036
Tel: (202) 282-5276
Email: beferguson@winston.com

Rex A. Mann
WINSTON & STRAWN LLP
2121 North Pearl Street, Suite 900
Dallas, TX 75201
Tel: (214) 453-6500
Email: rmann@winston.com

Attorneys for Core Scientific, Inc.

**CERTIFICATE OF COMPLIANCE WITH THE COURT'S
35 U.S.C. § 101 MOTION PRACTICE ORDER**

_____ The parties **agree** that prior claim construction is not needed to inform the Court's analysis as to patentability.

 X The parties **disagree** on whether prior claim construction is not needed to inform the Court's analysis as to patentability.

/s/ Brian E. Ferguson
Brian E. Ferguson

CERTIFICATE OF SERVICE

I certify that a true and correct copy of the foregoing document has been served on counsel of record, who are deemed to have consented to electronic service, on July 20, 2025, via electronic filing using the Court's CM/ECF system.

/s/ Brian E. Ferguson

Brian E. Ferguson